AMENDMENTS TO THE SPECIFICATION

On page 3 of the specification, please amend the paragraph beginning on line 3 as follows:

A PC and associated UE are used to register with a registration web server on the Internet Network via an ~~anonymous~~ open connection to the network including downloading subscriber identity information from the registration web server to the PC via the UE for storage in the PC. The subscriber identity information includes, at least, a unique user identification (user ID) and a permanent password. Such stored information constitutes a virtual subscriber identity module (VSIM). The access operator authentication server is updated with the user ID and password. The user may then be connected to an allowable Internet service provider (ISP) using the VSIM. Another PC may be used by transferring electronically the user ID and password to the other PC ~~said transfer including one of the following; temporary transfer to~~ via a portable magnetic storage means, a local area network (LAN), an [[or]] e-mail attachments, or ~~similar~~ an electronic ~~transfer~~ transferable file.

On pages 3 and 4 of the specification, please amend the paragraph beginning on line 19 as follows:

Referring now to FIG. 1, there is illustrated a wireless access user [[22]] with user equipment (UE) 22 connected by a typical data connection to the personal computer (PC). The personal computer has a CD drive or similar media input device with a special compact disc containing software, including a wizard (that is the instructional system procedures for registration) which is placed in the CD drive. In addition, a second PC and UE 21 is illustrated ~~designated~~, a new PC whose function in the Internet Network system shown in FIG. 1 will be described below.

On page 5 of the specification, please amend the paragraph beginning on line 3 as follows:

In all cases of communication of a user equipment 21 or 22 through the Internet Protocol Network, illustrated as 31, authentication is performed by the user equipment (UE) signaling the customer's wireless access authentication information which is passed over the air to Integrated Network Controller 24 which queries a RADIUS ~~server~~ authentication server with the user ID (identification) and temporary password. The RADIUS server used is the Access Operator's RADIUS Authentication Server 34 which communicates with the Integrated Network Controller via the IP network using UDP/IP protocols with additional protocol layers for sercurity.

On page 5 of the specification, please amend the paragraph beginning on line 20 as follows:

Thus, the foregoing constitutes the ~~anonymous~~ open session link where a general or non-authenticated user can still gain access to the wireless access operator's registration server for the purpose of new-user registration. The accompanying legend indicates the various paths. A UMTS access network 33 operator [[33]] provides the special servers 34 and 36 along with the billing system 37.

On pages 5 and 6 of the specification, please amend the paragraph beginning on line 25 as follows:

The flow chart of FIG. 3 describes in somewhat truncated detail the registration procedure set out in greater detail in the above co-pending '699 application. After "START" in Step 1, the user purchases the user equipment UE which may or may not have a particular unique identification number (ID) and a CD with the appropriate software and wizard feature installed on it. This is connected to the PC. Next in Step 2, the user equipment is installed on the PC via the wizard instructions on the CD, along with a new user ID and temporary password which were contained on the CD. These are then sent to the UE. The UE sends this authentication information over the air to the RNC 26, which is passed onto the RADIUS Client 29 and the SGSN 27 which queries the RADIUS server 34 with a new user ID and temporary new user password. In effect, an ~~anonymous~~ open connection using the temporary password is made on the Internet and as described in the above co-pending application, a permanent password is generated along with a user ID. As indicated in Step 3, this is stored in the PC memory of the unit 22. Thus, the permanent password and ID which have been electronically stored in the PC memory (which may be a randomly accessible memory or floppy disk or hard disk) form a virtual subscriber identity module or VSIM. At the same time (Step 6), the RADIUS server 34 is updated with the user's name and permanent password to provide subsequent access to allowable ISPs 40, as illustrated in FIG. 1. Thus, as described in the above co-pending application, access has been gained to the Internet Network on a special ~~anonymous~~ open connection. Thus, as described in Step 4, connection may now be made to allowable Internet service providers (ISPs) using the VSIM user information via the Layer 2 Tunneling Network Server (LNS) 45 of the allowable ISPs 40. This route is shown in a dashed line designated End User Traffic 46.

On page 6 of the specification, please amend the paragraph beginning on line 22 as follows:

With the VSIM, in accordance with the present invention, as shown in Step 6, a user may electronically transfer the subscriber identity information to a new or another PC, for example, indicated as 21 in FIG. 1. This is illustrated in FIG. 2 where the original PC 22 with the VSIM subscriber identity module information indicated in dashed outline transfers the VSIM information via one of the following electronic techniques so designated: floppy disk, LAN (Local Area Network), e-mail attachment or other electronic means. Thus, the new PC 21 contains the VSIM information so designated in the dashed block as [[VISIM]] VSIM and may access the Internet Network. Optionally, if as part of the VSIM or subscriber identity information, the unique identification or ID of the ~~original~~ associated UE with PC 22 is part of the VSIM information, then as shown by the optional line 47 the ~~original or old~~ UE must be transferred to the new PC 21. This prevents use by more than one subscriber; in other words, it is further protection against fraud. However, this is not necessary if the user equipment ID is not a part of the required VSIM information.